



**Privacy Impact Assessment Update
for the**

**HSIN R3 User Accounts: Service
Provider within the National Information
Exchange Federation (NIEF)**

DHS/OPS/PIA-008(d)

August 28, 2014

Contact Point

James Lanoue

DHS Operations Coordination and Planning

HSIN Program Management Office

(202) 343-4224

Reviewing Official

Karen Neuman

Chief Privacy Officer

Department of Homeland Security

(202) 343-1717



Abstract

The Department of Homeland Security (DHS), Office of Operations Coordination and Planning (OPS) maintains the Homeland Security Information Network (HSIN). HSIN is designed to facilitate the secure integration and interoperability of information-sharing resources among federal, state, local, tribal, private-sector, and other non-governmental stakeholders involved in identifying and preventing terrorism as well as undertaking incident management activities.¹ This Privacy Impact Assessment (PIA) Update documents how OPS established new information sharing relationships under the National Information Exchange Federation (NIEF). This PIA details HSIN's new capability as a Service Provider within NIEF and with the Regional Information Sharing System (RISSNET) Program.

Overview

HSIN is a user-driven, web-based, information-sharing platform that connects all homeland security mission partners within a wide spectrum of homeland security mission areas. DHS mission partners rely on HSIN as a trusted environment that supports DHS missions by: 1) providing timely and accurate information related to detecting, preventing, responding to, and recovering from terrorist attacks and natural disasters; 2) providing timely and accurate information regarding vulnerabilities and threats, managing incidents to mitigate risks, and reducing post-incident loss of life and property; 3) providing near-real time collaboration and incident management; 4) facilitating information exchange for emergency management response and recovery operations; and 5) connecting disparate information users in a dynamic and diverse information exchange environment.

The DHS/OPS/PIA-008(c) HSIN R3 User Accounts: Identity Provider within the National Information Exchange Federation (NIEF) PIA² provides an overview of federation principles, trust frameworks, and the federal governance processes around federation. The same principles and regulations about federation apply to this updated PIA. This PIA update describes HSIN as not only an Identity Provider, but now a Service Provider within NIEF.

NIEF is a collection of agencies in the U.S. that have come together to share sensitive law enforcement information.³ A federation is the technology, standards, policies, and processes that allow an organization to trust digital identities, identity attributes, and credentials created and

¹ For a detailed description of the HSIN program generally and the associated privacy risks, please *see* DHS/OPS/PIA-007 – HSIN 3.0 Shared Spaces on the Sensitive But Unclassified Network PIA, *available at* http://www.dhs.gov/sites/default/files/publications/privacy/privacy_pia_ops_hsin_sharespace_07252012.pdf and the DHS/OPS/PIA-008 HSIN R3 User Accounts PIA and subsequent updates, *available at* <http://www.dhs.gov/privacy-documents-office-operations-coordination-and-planning>.

² DHS/OPS/PIA-008(c) - HSIN Release 3 User Accounts: Identity Provider within the National Information Exchange Federation, *available at* <http://www.dhs.gov/sites/default/files/publications/privacy-pia-update-ops-hsin-r3-user-accounts-interop-federation-february2014.pdf>.

³ For more information, please visit the National Identity Exchange Federation, *available at* <https://nief.gfipm.net/>.



issued by another organization. Federated information access with NIEF allows HSIN to enable, operate, maintain, enhance, and expand the secure, standards-based, inter- and intra-Departmental information sharing through the globally recognized Global Federated Identity and Privilege Management (GFIPM) standard.⁴

Federated Identity Management Roles⁵

In this federated information sharing model identity credentials issued to a user by a particular service or entity are recognized by a broad range of other systems. A trust-enabled federation typically contains the following roles:

- **Relying Party (RP), or Service Provider (SP):** A web application that provides a service to the user, but has outsourced user authentication. This service thus “relies” on a third party to provide identity information.
- **Identity Provider (IdP):** An approved organizational entity with which the user has established his or her identity in accordance with OMB Memo 04-04 (E-Authentication guidance for Federal Agencies)⁶ and NIST 800-63-1 (Electronic Authentication Guideline).⁷ The IdP provides identity verification services to the RP/SP.
- **Discovery Service:** A means of finding an IdP that is acceptable to both the user and the RP/SP; this could be as simple as a drop-down menu on the RP/SP’s website.

HSIN as a Service Provider within NIEF

HSIN is already operating as an IdP within NIEF with RISSNET. This PIA addresses an update to the environment, wherein HSIN will now act as an RP/SP, allowing RISSNET users to access HSIN data without a separate log-on process. Thus, when a RISSNET user accesses HSIN, only the information required for the user to operate within HSIN is exchanged from RISSNET to HSIN during this transaction. Further information about NIEF, the Security Assertion Markup Language (SAML) data exchange, and a sample federation scenario can be found in the DHS/OPS/PIA-008(c) HSIN R3 User Accounts: Identity Provider within the National Information Exchange Federation (NIEF) PIA.

The benefits of HSIN operating as an RP/SP within NIEF means that HSIN does not need to provide full identity verification and credentialing services to NIEF users. This will save

⁴ GFIPM standards, *available at* <http://www.gfipm.net/deliverables/standards/>.

⁵ A federated identity is an identity system that allows the sharing of identity credentials, and for identity information to be asserted, by one or more identity providers, with multiple relying parties and trusted partners. *See* American Bar Association Identity Management Legal Task Force Confidential Discussion DRAFT, Solving the Legal Challenges of Online Identity Management PART 1 Identity Management Fundamentals and Terminology, December 30, 2011.

⁶ OMB Memo M-04-04, E-Authentication Guidance for Federal Agencies, *available at* <http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf>.

⁷ NIST 800-63-1, Electronic Authentication Guideline, *available at* <http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf>.



HSIN time, resources, and cost by leveraging existing trust relationships, governance, and processes implemented by NIEF to trust and accept identities asserted from NIEF IdPs, in this case RISSNET.

Additional benefits of joining NIEF as an RP/SP include an increased user base for HSIN and its community. The benefits from operating as an RP/SP within NIEF affects more than 95,000 users representing various criminal justice-related organizations who can access information resources (subject to the specific RP/SPs access control policy) without requiring the RP/SP to manage any additional user accounts.

Reason for the PIA Update

DHS is updating this PIA because HSIN is now serving as Service Provider within NIEF. This means that HSIN will now accept external users whose identities have been authenticated by a third party – in this case, RISSNET.

HSIN will allow users to use credentials issued by their organization to authenticate security to HSIN as the network continues to expand. This update specifically covers users with a RISSNET account accessing HSIN without being asked to provide another user name or password. This technique is called “Identity Federation” and is based on industry security standards such as Public Key Infrastructure (PKI) and SAML. HSIN will trust RISSNET identities and allow their users to access HSIN without prompting them for new user names or passwords. However, HSIN may ask the user or RISSNET to provide additional information about the user since HSIN may require more information than RISSNET maintains to establish a HSIN account.

This capability (also known as Service Provider) is the exact inverse of the capability introduced in HSIN earlier in 2014, as described in the DHS/OPS/PIA-008(c) HSIN Release 3 User Accounts: Identity Provider within the National Information Exchange Federation PIA. HSIN users can currently access RISSNET with their HSIN account. The trust established to do this is exactly the same as what will be used to accept RISSNET accounts into HSIN.

Privacy Impact Analysis

In each of the below sections consider how the system has changed and what impact it has on the below fair information principles. In some cases there may be no changes and indicate as such.

Authorities and Other Requirements

Authorities have not changed from the original HSIN PIA. Of note, DHS recently established the DHS/ALL-037 E-Authentication Records System of Records to account for the collection and maintenance of information associated with enrolling, issuing, and maintaining credentials (e.g., online account) for individuals seeking electronic access to DHS programs, services, and applications including when DHS uses a trusted third-party identity service



provider.⁸ HSIN's collection and management of user attributes is now covered by the DHS/ALL-037 E-Authentication Records SORN.

Characterization of the Information

In its new role as a Service Provider in NIEF, HSIN is collecting five (5) additional attributes:

- Federation ID
- User Distinguished Name (DN)
- FASC-N (Federal Agency Smart Credential Number)
- Accept Terms of Service
- Sworn Law Enforcement Officer Indicator

All user attribute information previously documented by the original DHS/OPS/PIA-008 HSIN R3 User Accounts PIA,⁹ updated with the five (5) new user attributes, are detailed in Appendix A.

The five new attributes are obtained from: the SAML assertion from RISSNET, the user's acceptance of HSIN's Terms of Service, or the user's Personal Identity Verification (PIV) credential. Attributes asserted by RISSNET are collected and vetted by RISSNET, including Federation ID and Sworn Law Enforcement Officer (SLEO) Indicator. The new attributes are described as follows:

Attribute	Description	Attribute Detail
Federation ID	The persistent, federation-unique identifier for the user comprised of a federation part, an optional trusted broker part, identity provider (IdP) part, and a local ID part.	Identity provider implemented attribute that uniquely identifies a user from a federated partner.
USERDN	The unique identifier of the user associated with the user's Personal PIV card.	The identifier includes the person's common name, organization, organizational unit, and country code.

⁸ DHS/ALL-037 E-Authentication System of Records, 79 FR 46857 (August 11, 2014), available at <http://www.gpo.gov/fdsys/pkg/FR-2014-08-11/html/2014-18703.htm>.

⁹ DHS/OPS/PIA-008 HSIN R3 User Accounts PIA, available at http://www.dhs.gov/sites/default/files/publications/privacy/privacy_pia_ops_hsin_r3useraccounts_07252012.pdf.



FASCN	FASC-N (Federal Agency Smart Credential Number), which uniquely identifies each Personal Identity Verification (PIV) card.	The FASC-N incorporates credibility, non-repudiation, and reciprocity, to uniquely identify each user so as to provide secure access management and physical access rights and privileges to users at Federal Government facilities and Federal Government secure information systems.
Accept Terms of Service	This is an indicator that the user has read and accepted the HSIN Terms of Service (TOS).	If the user does not accept the HSIN TOS, then the user is denied access to HSIN.
Sworn Law Enforcement Officer Indicator	<p>The user is a full time employee of a state-recognized law enforcement agency who is an authorized to make an arrest, or user certified by a State Certifying Authority (i.e., Peace Officer Standards and Training (POST)), or equivalent.</p> <p>The user is a SLEO if the user is a full time employee of a state-recognized law enforcement agency, acting on behalf of a SLEO, in performance of the user's assigned duties.</p>	This attribute indicates the user has been verified to be a SLEO or has a role in supporting a SLEO and may be granted access to law enforcement sensitive information.

DHS does not have access to commercial identity verification information. Third-party identity service providers use a variety of verification techniques, commensurate with M-11-11¹⁰ and NIST SP 800-63¹¹ including knowledge-based authentication to generate a quiz containing questions that only the individual should be able to answer. The quiz is based on commercial identity verification information collected by companies from financial institutions, public

¹⁰ OMB Memo M-11-11, "Continued Implementation of Homeland Security Presidential Directive (HSPD) 12—Policy for a Common Identification Standard for Federal Employees and Contractors," (February 3, 2011), available at <http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf>.

¹¹ NIST Special Publication 800-63, "Electronic Authentication Guideline," (August, 2013), available at <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf>.



records, and other service providers. Information accessed by the third-parties includes information such as the individual's commercial transaction history, mortgage payments, or past addresses. DHS does not have access to the commercial identity verification information, the quiz questions asked of the individual, or the responses provided thereto; therefore this commercial information is not included in the DHS/ALL-037 E-Authentication System of Records Notice. DHS receives assertions (e.g., pass or fail) and assertion references (e.g., transaction ID, date/time of the transaction, error codes) from the identity service provider to facilitate troubleshooting and system management.

The changes specified in this PIA are related to the five new attributes identified in the above sections. RISSNET asserts two of these attributes to HSIN under the guiding principles of NIEF. As such, RISSNET (acting as an approved IdP in NIEF) has implemented technology and processes to provide the accuracy of the data collected and stored about its users. RISSNET asserts these attributes to HSIN, which trusts that the attributes are accurate under the NIEF governance framework.

New risks based on HSIN's collection of new attributes from RISSNET include:¹²

Privacy Risk: There is a risk that the attributes provided by RISSNET about the user are not valid.

Mitigation: RISSNET is a member of NIEF and as such must abide by its rules and regulations, including applicable OMB and NIST standards. HSIN trusts the Identity Providers that are a part of NIEF. Additionally, HSIN has an MOU developed directly with RISSNET outlining the roles and responsibilities of the two parties in exchanging data between each other.

Uses of the Information

HSIN is now serving as Service Provider within NIEF. HSIN will use the additional five attributes collected to uniquely identify a RISSNET or DHS PIV user, validate his or her identity, and authorize access to HSIN applications. In some cases these users create their own HSIN account; however, HSIN will allow users to use credentials issued by their organization to authenticate security to HSIN as the network continues to expand. This technique is called "Identity Federation" and is based on industry security standards such as PKI and SAML.

HSIN will trust RISSNET identities and allow their users to access HSIN without prompting them for new user names or passwords. However, HSIN may ask the user or RISSNET to provide additional information about the user since HSIN may require more information than RISSNET maintains to establish a HSIN account. DHS decreases the burden on its users and costs associated with managing credentials by permitting individuals to choose

¹² Note the previous privacy risks identified in earlier updates for DHS/OPS/PIA-008 R3 User Accounts are still applicable.



to reuse his or her credential obtained for one or more programs within DHS or elsewhere in the Federal Government with the individual's consent.

The risks, mitigations, and technical controls identified in the DHS/OPS/PIA-008 HSIN R3 User Accounts PIA sufficiently address the uses of information for the new attributes. The new attributes collected as part of this PIA are governed and protected in the same fashion as other attributes within HSIN. In addition, HSIN abides by the NIEF governance framework and has established an MOU with RISSNET describing the roles, responsibilities, and intended use of the respective systems.

Notice

DHS established the DHS/ALL-037 E-Authentication Records System of Records to account for the collection and maintenance of information associated with enrolling, issuing, and maintaining credentials (e.g., online account) for individuals seeking electronic access to DHS programs, services, and applications including when DHS uses a trusted third-party identity service provider. HSIN's collection and management of user attributes is now covered by the DHS/ALL-037 E-Authentication Records SORN.

When a user reads and accepts the HSIN Terms of Service the user is given notice of which attributes are collected and how they are used. This includes notice that the user's information will not be sold to any social media site, or other commercial entity. No additional notice is required because federation and PIV authentication users must accept the HSIN Terms of Service in order to be granted access to the HSIN Information Sharing platform. The HSIN Terms of Service includes acceptable use and what user information is collected, retained, and how it is used.

Data Retention by the project

Records are securely retained and disposed of in accordance with the NARA's General Records Schedule (GRS) 24, section 6, "User Identification, Profiles, Authorizations, and Password Files." Inactive records are destroyed or deleted six years after the user account is terminated or password is altered, or, on limited occasion, when no longer needed for investigative or security purposes. DHS retains the records for this time to ensure effective and efficient administration of the registration process over time, and to comply with any potential audit, legal, or investigative requirements that may arise in the normal course of the homeland security information environment's business.

In addition, in accordance with NIST SP-800-63-2, a record of the registration, history, and status of each token and credential (including revocation) is maintained by HSIN. While the identity record itself may not be retained beyond six years, if it is inactive or revoked, credential data may be maintained longer in order to comply with NIST requirements. Specifically, the record retention period of data for Level 2 and 3 credentials is seven years and six months beyond the expiration or revocation (whichever is later). The minimum record retention period



for Level 4 credential data is ten years and six months beyond the expiration or revocations of the credential. The risks, mitigations, and technical controls identified in the DHS/OPS/PIA-008 HSIN R3 User Accounts PIA sufficiently address the retention of the new attributes for this PIA.

Information Sharing

There are no changes to the internal sharing and disclosure procedures described in the HSIN User Accounts PIA.

Redress

Redress procedures have not changed from previously published PIA versions. However, HSIN R3 User Account information is now covered under the newly established DHS/ALL-037 E-Authentication Records System of Records Notice. Users may follow the same access, correction, and amendment procedures described under previous PIA versions, or as described in the new SORN.

Auditing and Accountability

There are no changes to how the user information is used for authentication and authorization purposes in granting/receiving access to HSIN resources or disclosure procedures as described in the DHS/OPS/PIA-008 HSIN R3 User Accounts PIA. All HSIN personnel maintain standard DHS awareness training, including DHS Privacy Awareness training, which is available to all HSIN users, including RISSNET users.

There are no changes to the internal sharing and disclosure procedures described in the DHS/OPS/PIA-008 HSIN R3 User Accounts PIA.

Responsible Official

James Lanoue
HSIN Program Manager
Office of Operations Coordination and Planning
Department of Homeland Security

Approval Signature

Original signed copy on file with DHS Privacy Office

Karen Neuman
Chief Privacy and FOIA Officer
Department of Homeland Security



Appendix A

Full list of User Attribute Information Collected and Maintained by HSIN R3:

Information Collected	Included in the Original R3 User Accounts PIA?
FederationID	No
UserDN	No
FASCN	No
Accept Terms of Service	No – Information collected in the Terms of Service is not PII
Sworn Law Enforcement Officer Indicator	No
First Name	Yes
Middle Initial	Yes
Last Name	Yes
Primary E-mail	Yes
Phone Number	Yes
U.S. Citizenship	Yes
Security Question	Yes
Security Answer	Yes
OTP – Email	Yes
OTP – SMS	Yes
OTP – IVR	Yes
Organization	Yes
Display Name	Yes
Job Title	Yes
Users Assigned Agency	Yes
Supervisor Name	Yes
Supervisor Telephone Number	Yes
Supervisor Email Address	Yes
Supervisor Organization	Yes